Report Date: 23 Nov 2016
Summary Report for Staff Drill Task
Drill Number: 71-DIV-D7176
Drill Title: React to Jamming or Suspected Communications Compromise (Battalion through Division)
Status: Approved
Status Date: 21 Nov 2014

Distribution Restriction: Approved for public release; distribution is unlimited.
Destruction Notice: None
Foreign Disclosure: FD1 - This training product has been reviewed by the training developers in coordination with the Fort Leavenworth foreign disclosure officer. This training product can be used to instruct international military students from all approved countries without restrictions.

Drill Data
Proponent: 71 - Combined Arms (Collective)
Drill Type: Staff
Approved: 21 Nov 2014
Obsolete:
Restricted Read: No
Route To TMD Reviewer: Yes
TMD Concurrence: Yes
TMD Comments: Concur: Comments fixed

Safety Level: Low

Conditions:

The command reacts to a jamming or a suspected communications compromise. The command establishes communications with higher, lower, and adjacent units, and the mission command system is operating and processing information. The commander issues guidance on reacting to threats to communication capabilities. Perform some iterations of this drill during limited visibility. Some iterations of this task should be performed in MOPP 4.

MOPP 4 Statement:

Standards:

The staff reacts to jamming or communications compromise following commanders guidance and standard operating procedures. The staff takes appropriate steps to resolve problems at the local level and to protect mission command systems. The staff maintains continuous communications throughout operations.

Drill Statements:

WARNING

Proper utilization of the Risk Assessment and unit SOP to lower the risk level.

Safety: In a training environment, leaders must perform a risk assessment in accordance with ATP 5-19, Risk Management. Leaders will complete the current Deliberate Risk Assessment Worksheet in accordance with the TRADOC Safety Officer during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection, FM 3-11.5, Multiservice Tactics, Techniques,

and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination.

Environment: Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to the current Environmental Considerations manual and the current GTA Environmental-related Risk Assessment card. Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT. .

Cue: The staff recieves a report of jamming or suspecting communications compromise.

Coaching Point: Validate the SOP is current and the staff is familiar with the performance measure within this drill.

TASK STEPS

1. The staff reacts to jamming or communications compromise by employing all electronic warfare (EW) elements: electronic warfare support (ES), electronic attack (EA), and electronic protection (EP).

2. The staff employs ES by:

a. Searching for, interrupting, locating, recording, and analyzing radio signals for using such signals in support of military operations.

b. Providing EW information required to combat electronic countermeasures, to include threat detection, warning, avoidance, target location, and homing.

c. Producing signals intelligence (SIGINT), communications intelligence, and electronic intelligence.

3. The staff employs EA by:

a. Employing electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading.

b. Preventing or reducing the enemy's effective use of his frequencies, which includes jamming and deception.

c. Employing weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency (RF) weapons, and particle beams).

4. The staff employs EP by:

a. Ensuring friendly effective use of frequencies, despite enemy's use of EW.

b. Coordinating the use of the electromagnetic spectrum through the joint restricted frequency list (JRFL).

c. Providing defensive measures used to protect friendly systems from enemy EW activities, including but not limited to:

(1) Careful siting of radio equipment.

(2) Employment of directional antennas.

(3) Using lowest power required.

(4) Staying off the air unless absolutely necessary.

(5) Employing a random schedule if one is used.

(6) Using good radio techniques and continuing operation.

(7) Employing proper radio techniques and continuing operation.

5. The staff employs remedial EP techniques to react to jamming or suspected communication interference by:

a. Identifying jamming signals.

b. Determining if the interference is obvious or subtle jamming.

c. Verifying jamming or compromise by ruling out causes such as:

(1) Equipment problems.

(2) Non-existent and/or invalid frequency assignments.

(3) Natural phenomenon (space or weather).

d. Recognizing jamming and interference by:

(1) Determining whether the interference is internal or external to the radio.

(2) Determining whether the interference is jamming or unintentional.

(3) Reporting jamming and interference incidents.

6. The staff defeats jamming and interference by adhering to the following techniques:

a. Continuing to operate, even when degraded by jamming.

b. Improving the signal-to-jamming ratio.

c. Adjusting the receiver.

d. Increasing the transmitter power output.

e. Adjusting or changing the antenna.

f. Establishing a wireless network extension station.

g. Directing an alternate route for communications.

h. Changing the frequencies.

i. Acquiring another satellite.

Leader Statement: The commander is the final decision maker on all electronic protection measures.

* 7. The commander employs electronic protection measures by:

a. Validating units train and practice sound EP techniques.

b. Reviewing all after action reports (AARs) of jamming or deception.

c. Validating the assistant chief of staff, signals (G-6) or signal staff officer (S-6) and the assistant chief of staff, intelligence (G-2) or intelligence staff officer (S-2) properly analyze all encounters of interference, deception, or jamming.

d. Analyzing the impact of enemy efforts to disrupt or destroy friendly command and control (C2) communications systems on friendly operations plans (OPLANs).

e. Validating the unit practices communications security (COMSEC).

8. The staff complies with all higher headquarters' regulations and guidelines for conducting cyber threat activities.

9. The staff briefs the commander on cyber threat activities and events.

10. The staff provides cyber threat reports and summaries to the commander and to higher, lower, and adjacent units.

(Asterisks indicates a leader performance step.)

TASK MEASURES

1. The staff reacted to jamming or communications compromise by employing all electronic warfare (EW) elements: electronic warfare support (ES), electronic attack (EA), and electronic protection (EP).
2. The staff employed ES.
3. The staff employed EA.
4. The staff employed EP.
5. The staff employed remedial EP techniques and reacted to jamming or suspected communication interference
6. The staff defeated jamming and interference by employing the correct techniques.
7. The commander directed the employment of electronic protection measures.
8. The staff complied with all higher headquarters' regulations and guidelines for conducting cyber threat activities.
9. The staff briefed the commander on cyber threat activities and events.
10. The staff provided cyber threat reports and summaries to the commander and to higher, lower, and adjacent units.

Talk:

a.Orientation: The objective of this drill is to react to jamming or suspected communications compromise without degradation to the mission.

b.Safety: Emphasize that following the SOP and EW protocols are critical for preventing compromise of the system.

c.Demonstration: Have the staff conduct a rehearsal of concept of the SOP.

d.Explanation: Refer to the performance measures and explain what each member of the staff must do to react to jamming or suspected communications compromise.

e.Unit Instructions: The Staff is coordinating current operations and receives a report of jamming or suspected communications compromise.

Walk:

1. Refer to the performance measures and have staff members perform their step slowly at first as the leader talks them through the process.
2. Continue to rehearse, increase speed of execution each iteration.

Run:

a.Run-Through Instructions: The staff should practice this drill until they can perform the drill according to the standards and without the drill book or coaching form the leader.

b.Coaching Point: Validate the SOP is current and the staff is familiar with the performance measure within this drill.

c.Performance Instructions: Rehearse this Drill IAW performance measures.

Equipment (LIN)

Step ID	LIN	Nomenclature	Qty
No equipment specified			

Materiel Items (NSN)

Step ID	NSN	LIN	Title	Qty
No materiel items specified				

Support Personnel

Personnel Type	Description	School	Qty	Remarks
No support personnel specified				

TADSS

Step ID	TADSS ID	Title	Product Type	Qty
No TADSS specified				

Supporting Individual Tasks

Step ID	Task ID	Status	Task Title
	011-240-1404	Approved	Perform Electronic Counter Measures (ECM)/Electronic Counter-Counter Measures (ECCM) Procedures (CH-47D/F)
	011-420-0031	Approved	Implement Operations in an Electronic Warfare Environment
	011-AMS-0004	Approved	Develop Aviation Mission Survivability (AMS) and Personnel Recovery (PR) Appendixes/Annexes to Plans and Orders
	150-029-0007	Approved	Produce Electronic Warfare Products in Support of the Military Decision Making Process (MDMP)

Prerequisite Individual Tasks

Step ID	Task ID	Status	Task Title
	011-410-0013	Superseded	Develop the Tactical Survivability Appendix of the Electronic Warfare Annex to Operation, Plans, and Orders (OPORD)
	011-420-2717	Approved	Implement Operations in an Electronic Warfare (EW) Environment

Supporting Collective Tasks

Step ID	Task ID	Status	Title
	34-4-0824	Approved	Conduct a Multifunctional Team Electronic Support Mission
	34-5-0800	Approved	Establish an Electronic Support (ES) or Electronic Attack (EA) Site
	71-8-6330	Approved	Perform Electronic Protection Actions (Brigade - Corps)

Prerequisite Collective Tasks

Step ID	Task ID	Status	Title
	11-5-0106	Superseded	Conduct Communication Security (COMSEC) Logistic Support
	71-8-3501	Approved	Coordinate Electronic Warfare (Brigade - Corps)
	71-8-3502	Approved	Assess Electronic Warfare Operations (Brigade - Corps)
	71-8-6330	Approved	Perform Electronic Protection Actions (Brigade - Corps)

Supporting Drill Tasks

Step ID	Drill ID	Status	Drill Title
No supporting drill tasks specified			

OPFOR

Task Number	Title	Status
No supporting OPFOR tasks specified		

REFERENCES

Step Number	Reference ID	Reference Name	Required	Primary
	ATP 6-02.53	Techniques for Tactical Radio Operations	Yes	No
	FM 3-36	Electronic Warfare in Operations	Yes	Yes
	FM 6-0 (Change 002, April 22, 2016)	COMMANDER AND STAFF ORGANIZATION AND OPERATIONS	Yes	No

Training Setup

Table (s) of organization and equipment (TOE) assigned personnel and equipment; weapons; vehicles; and communication equipment/mission command systems.

Training Facilities

Facility ID	Facility Name	Facility Type
No Training Facilities		

DODIC

DODIC	Name	Qty
No DODIC		

Associated Documents

Media ID	Media Type	Title	Subtitle
No Associated Documents			

GLOSSARY TERMS

Glossary Term	Definition
electronic attack	(DOD) That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1. actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2. employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams), or antiradiation weapons. See also electronic warfare;information operations. See FM 34-1.
electronic protection	(DOD) That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize or destroy friendly combat capability. Also called EP. See also electronic warfare. See FM 34-1
electronic warfare support	(DOD) That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. See also electronic warfare. See FM 34-1.

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	Definition
EP	electronic protection; EPLRS Planner; electrophysiology; exposure points; Engagement Planner
ES	electronic warfare support
EW	early warning;electronic warfare